Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 1301-1307

PERTANGGUNGJAWABAN PIDANA ATAS PENYALAHGUNAAN HAK AKSES DIGITAL TERHADAP DATA PELAKU USAHA DALAM SISTEM ELEKTRONIK *ONLINE SINGLE SUBMISSION* (OSS) BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022

Anes Sefta Asmita
Ilmu Hukum, Hukum, Universitas Sriwijaya
Email : anessefta@gmail.com

Informasi

Volume : 3
Nomor : 7
Bulan : Juli
Tahun : 2026
E-ISSN : 3062-9624

Abstract

The advancement of digital technology is something that should be welcomed positively, especially digital technology progress in public services, which is certainly very beneficial to the community. Currently, there is a digital system known as "Online Single Submission" or OSS, which is used by business actors to fulfill their administrative process obligations. Business actors have the obligation to enter personal data and other documents related to the fulfillment of business administrative obligations into a state-owned "Online Single Submission" system. In practice, criminal acts related to the protection of personal data have been found, namely the abuse of digital data access rights of business actors caused by authorized officials in the bureaucratic process. This study aims to analyze the characteristics of digital access rights abuse associated with field cases regarding licensing extortion originating from the digital data access rights of business actors within the OSS system, whose validation or verification processes are hampered by perpetrators or rogue officials. The digital licensing data that is intentionally hampered constitutes an administrative violation, and then formulates the administrative criminal law liability for public officials who abuse digital access rights. The research method used is normative juridical with a statute approach and a conceptual approach. The results of the study indicate that the abuse of digital access rights in the OSS system leads to criminal acts, namely extortion and corruption. The legal obligation of supervision is mandated in Articles 14 to 16 of Law Number 27 of 2022 concerning Personal Data Protection. The criminal acts committed by officials in abusing data access rights within the OSS system constitute a form of criminal offense regulated under the Personal Data Protection Law. The reference case in this study is the case of I Made Kuta, who served as the Head of the One-Stop Integrated Investment and Services Office (DPMPTSP) of Buleleng, who abused access rights to business actors' data using his data access rights to access data in the OSS system for the primary purpose of committing extortion. However, the main highlight of this case is that I Made was only subjected to sanctions for extortion and was not sanctioned for the abuse of office specifically, the violation regarding business actors' personal data access rights which also breaches the Personal Data Protection Law. Ideal law enforcement must accumulate all committed criminal acts. In other words, the act of abusing data access rights in the OSS system held by officials needs to be addressed in order to guarantee legal certainty, restore public trust, and protect the constitutional rights

of data owners within the digital system, namely the "Online Single Submission" (OSS).

***Keywords**: Abuse of Data Access Rights, OSS System, Administrative Criminal Law*

Abstrak

*Kemajuan Teknologi digital adalah sesuatu yang sudah seharusnya disambut dengan positif terutama kemajuan teknologi digital dalam pelayanan publik yang tentu sangat bermanfaat bagi masyarakat. Saat ini dikenal sistem digital yang bernama "*Online Single Submission*" atau OSS yang digunakan oleh pelaku usaha dalam kewajiban proses administrasi. Pelaku usaha memiliki kewajiban untuk memasukkan data pribadi dan dokumen lain yang berkaitan dengan pemenuhan kewajiban administrasi usaha dalam suatu system "Online Single Submission" yang dimiliki negara. Dalam Praktiknya ditemukan tindak pidana terkait perlindungan data pribadi yaitu adanya penyalahgunaan hak akses digital data pelaku usaha yang disebabkan oleh pejabat yang berwenang dalam proses birokrasi. Penelitian ini bertujuan untuk menganalisis karakteristik penyalahgunaan hak akses digital dikaitkan dengan kasus di lapangan mengenai pemerasan perizinan yang bermula dari hak akses data digital pelaku usaha dalam sistem OSS yang dihambat proses validasi atau verifikasinya oleh pelaku atau oknum pejabat. Data perizinan digital yang sengaja dihambat adalah bentuk tindak pidana administrasi, kemudian merumuskan pertanggungjawaban hukum pidana administrasi bagi pejabat publik yang menyalahgunakan hak akses digital. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Hasil penelitian menunjukkan bahwa penyalahgunaan hak akses digital di sistem OSS yang berujung terjadinya tindak pidana yaitu pemerasan dan korupsi. Kewajiban hukum pengawasan diamanatkan dalam Pasal 14 sampai Pasal 16 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Tindak pidana yang dilakukan pejabat dalam menyalahgunakan hak akses data dalam sistem OSS merupakan suatu bentuk tindak pidana yang diatur dalam Undang-undang Perlindungan Data Pribadi. Kasus yang menjadi rujukan dalam penelitian ini adalah kasus I Made Kuta yang menjabat sebagai Kepada Dinas Pelayanan Modal Satu Pintu (DPMPTSP) Buleleng yang melakukan penyalahgunaan hak akses atas data pelaku usaha dengan hak akses data yang dia miliki untuk mengakses data di sistem OSS untuk tujuan utama melakukan tindak pidana pemerasan, namun yang menjadi sorotan dalam kasus ini adalah I Made Hanya dikenakan sanksi pemerasan tetapi tidak dikenakan sanksi atas tindakan penyalahgunaan jabatan yaitu hak atas akses data pribadi pelaku usaha yang juga melanggar Undang-undang Perlindungan data Pribadi. Penegakan hukum yang ideal harus mengakumulasi semua tindak pidana yang dilakukan dengan kata lain tindakan menyalahgunakan hak akses data dalam sistem OSS yang dimiliki pejabat menjadi hal yang juga perlu untuk dibahas guna menjamin kepastian hukum, memulihkan kepercayaan publik, serta melindungi hak konstitusional pemilik data dalam sistem digital yaitu "Online Single Submission" OSS.*

***Kata kunci**: Penyalahgunaan Hak Akses Data, Sistem OSS, Hukum Pidana Administrasi*

A. PENDAHULUAN

Indonesia adalah negara yang berdaulat oleh sebab itu senantiasa mengarahkan orientasi kebijakannya pada pencapaian kemakmuran masyarakat, yang manifestasinya terlihat nyata melalui modernisasi birokrasi berbasis teknologi informasi berupa sistem *Online Single Submission* (OSS). Inisiatif digital ini dihadirkan oleh pemerintah guna mengimplementasikan mandat konstitusional sebagaimana termaktub di dalam Pembukaan UUD 1945 untuk memangkas kerumitan birokrasi perizinan dunia usaha lewat penerapan

prinsip keterbukaan informasi. Kendati demikian, implementasi di lapangan justru memperlihatkan distorsi struktural berupa celah penyalahgunaan kewenangan atas kerahasiaan data pengusaha oleh oknum pejabat berwenang, yang berisiko memicu praktik pemerasan dan melanggar ketentuan Pasal 65 juncto. Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Undang-Undang Nomor 27 Tahun 2022).

Akar permasalahan mendasar dari anomali ini terletak pada disharmoni antara modernisasi sistem perizinan digital dengan rendahnya integritas aparatur pelaksana yang memegang kendali penuh atas basis data pelaku usaha (Suhdi, 2022). Tindak pidana di bidang pelindungan data pribadi menjadi bagian penting dalam bahasan hukum pidana administrasi, di mana penegakan hukum pidana administrasi (*administrative penal law*) dituntut tidak hanya memberikan sanksi administratif tetapi juga sanksi pidana guna memperbaiki celah kecurangan dalam pemanfaatan sistem OSS.

Penjatuhan hukuman pidana terhadap pelanggaran administratif terkait kerahasiaan informasi personal sudah semestinya mampu melahirkan efek jera secara nyata sekaligus membendung potensi keberulangan perbuatan serupa oleh aparatur negara lainnya. Ketentuan yuridis di dalam Pasal 67 UU No. 27 Tahun 2022 yang menetapkan ancaman hukuman penjara lima tahun serta denda sejumlah Rp5.000.000.000 wajib dieksekusi secara konsisten dan tanpa kompromi demi menjamin tegaknya supremasi hukum pelindungan data pada pemanfaatan sistem OSS (Farah, 2021).

Penyalahgunaan data akibat kepemilikan hak akses ke sistem OSS terkait teknis perizinan merupakan hal yang harus diwaspadai secara ketat, sehingga diperlukan pengawasan intensif atau pembentukan unit pengawas pelindungan data yang independen. Penguatan sistem pengawasan ini krusial untuk memastikan bahwa tidak ada celah bagi aparatur birokrasi untuk menyalahgunakan posisi dan kewenangannya dalam mengelola data digital pelaku usaha (Muslim, 2020).

Penyalahgunaan kewenangan atas pengelolaan informasi personal serta berkas teknis milik pengusaha oleh aparatur birokrasi di dalam ekosistem OSS secara doktrinal dikategorikan sebagai pelanggaran hukum administratif yang menabrak ketentuan hukum pelindungan data pribadi. Proses peradilan tidak boleh berhenti pada penjatuhan hukuman administratif internal semata, melainkan wajib mengeksekusi sanksi pidana melalui asas primum remedium sebagai langkah strategis untuk menciptakan efek jera bagi setiap pelaku kejahatan pembajakan data.

Modus operandi dalam tindak pidana penyalahgunaan hak akses data pribadi dalam sistem OSS yang dilakukan pihak berwenang umumnya berkaitan dengan validasi data pelaku usaha, yang dilakukan dengan cara menggantung atau menghambat verifikasi data secara melawan hukum. Tindakan semacam ini secara jelas mengingkari hak-hak subjek data pribadi dan tidak memenuhi unsur pengecualian yang diatur secara limitatif dalam Pasal 15 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Fakta di lapangan menunjukkan bahwa pihak yang memegang tonggak kepentingan sering kali sengaja mencari celah dengan menyalahgunakan hak atas akses data untuk berujung pada tindakan pemerasan, di mana data rahasia pelaku usaha dibuat menggantung atau dihambat proses validasi akunnya. Kondisi ini mempertegas urgensi penerapan Pasal 65 ayat (2) juncto. Pasal 67 ayat (2) Undang-Undang Pelindungan Data Pribadi secara konsisten guna melindungi hak konstitusional masyarakat dan mengembalikan integritas layanan publik berbasis digital (Undang-undang Nomor 27 Tahun 2022).

B. METODE PENELITIAN

Kajian ini menggunakan pendekatan yuridis normatif (doktrinal) yang sepenuhnya berbasis kepustakaan (*library research*) tanpa melibatkan riset lapangan, dengan menitikberatkan pada penelaahan ketentuan hukum positif dan asas-asas ilmu hukum terkait pertanggungjawaban yuridis terhadap pelanggaran administratif berupa eksploitasi wewenang akses informasi personal dalam ekosistem Online Single Submission (OSS). Pendekatan utama yang diterapkan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Bahan hukum yang dikaji terdiri atas bahan hukum primer, yakni Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta bahan hukum sekunder berupa literatur hukum, buku teks, jurnal ilmiah, dan doktrin terkait, di mana kasus nyata dari pemberitaan media massa hanya ditempatkan sebagai ilustrasi faktual atau rujukan penunjang untuk memperkuat konteks permasalahan yang dianalisis.

Prosedur perolehan seluruh bahan hukum tersebut ditempuh melalui penelaahan pustaka secara sistematis dan terarah. Selanjutnya, bahan-bahan hukum yang telah terkumpul dianalisis menggunakan metode deskriptif kualitatif secara normatif guna memberikan gambaran yang sistematis dan mendalam terhadap permasalahan yang diteliti. Tahap akhir dari penelitian ini dilakukan dengan menarik kesimpulan melalui pola penalaran deduktif, sehingga mampu menjawab rumusan permasalahan hukum secara komprehensif dan dapat dipertanggungjawabkan secara akademis.

C. HASIL PENELITIAN DAN PEMBAHASAN

Analisis Kasus

Data Pribadi atau dokumen yang menyangkut pribadi adalah data yang sangat dilarang untuk disalahgunakan, dengan melawan hukum untuk kepentingan seseorang dalam hal ini adalah pejabat. Data Pelaku usaha yang ditempatkan dalam Sistem Online Single Submission dillarang disalahgunakan oleh Pejabat Internal, sebagai suatu kerentanan penyalahgunaan wewenang secara aktif oleh oknum pejabat yang bekerja di institusi setempat, atau dapat juga dilakukan oleh atau melalui petugas administrator yang memiliki hak akses khusus (*privileged access*) ke dalam sistem.

Kasus Kepala Dinas PMPTSP Buleleng (I Made Kuta)

Pejabat Tinggi di Dinas Perizinan Buleleng secara sengaja menggunakan data-data permohonan administrasi proyek perumahan para pengusaha (data PKKPR/KKKPR dan PBG) yang masuk ke sistem perizinan untuk dihambat. Data tersebut dieksploitasi secara sengaja oleh pelaku untuk memeras para pengembang bersubsidi agar menyerahkan sejumlah uang demi kelancaran izin (I Made, 2025).

Undang-undang perlindungan Data Pribadi wajib membatasi akses data hanya untuk tujuan pelayanan publik yang sah. Ketika oknum pejabat yang sah membuka melihat atau dengan kata lain memiliki akses sehingga menggunakan data dokumen perizinan (yang memuat KTP/NPWP Pemohon) untuk tujuan lain yang melanggar Undang-undang perlindungan data Pribadi (bali.bpk.go.id).

I Made Juga melakukan tindakan menahan Validasi (*Hostage-Taking System*) untuk melancarkan tindakannya dilakukan kesengajaan akun perizinan proyek di sistem OSS dihambat, tindakan yang melanggar Pasal 65 ayat 1 dan 3 Undang-undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, yang melarang setiap orang menggunakan data yang bukan miliknya dengan cara melanggar hukum termasuk kedalamnya sengaja "menggantungkan akun pelaku usaha" atau menghambat proses data yang ada dalam sistem OSS (Antara News). Titik fokus yang akan dibahas pada penelitian ini mengenai Pertanggungjawaban Pidana Atas Kebocoran Data Pribadi Pelaku Usaha Dalam Sistem Elektronik Online Single Submission (OSS), Dalam penelitian ini yang akan dibahas bukan tindak pemerasan yang dilakukan I Made, Penelitian ini terfokus pada bagaimana pertanggungjawaban pidana jika yang menjadi instrumen awal penyalahgunaan hak akses data yang dilakukan oleh "pengendali" atau "*controller*" yang diberikan kewenangan atau akses terhadap data orang lain yang tersimpan dalam sistem OSS, I Made justru

menyalahgunakan kewenangannya untuk menahan validasi data pelaku usaha yang ada dalam sistem OSS, menggantung persetujuan dokumen digital seperti PKKPR/KKKPR dan PBG dalam sistem OSS Berbasis Risiko (Aryo, 2025).

Bentuk Pertanggungjawaban Pidana Pejabat yang Menyalahgunakan Hak Akses Digital Dengan Sengaja Menggantung Akun Pelaku Usaha

I Made Kuta sengaja melakukan Pelanggaran terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, tindakan pejabat yang sengaja menyalahgunakan hak akses digital untuk menggantung akun pelaku usaha dapat dijerat sanksi pidana karena melibatkan pemrosesan dan penggunaan data pribadi secara melawan hukum. Pejabat tersebut bertindak melampaui wewenangnya terhadap data pelaku usaha dan dapat dikenakan sanksi berdasarkan sesuai Pasal 67 ayat 3 Undang-undang Perlindungan Data Pribadi: yaitu Memanipulasi akses atau menangguhkan akun secara sepihak diancam pidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5 miliar (Undang-Undang Nomor 27 Tahun 2022).

Penguasaan Data Tanpa Hak

Pasal 67 ayat 1: Jika menggantung akun disertai penguasaan data secara ilegal untuk keuntungan pribadi dan merugikan pemilik, diancam pidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5 miliar.

Pidana Tambahan bagi Pejabat Publik Sesuai Pasal 69 Undang-undang Perlindungan Data Pribadi, pelaku dapat dijatuhi hukuman tambahan berupa Pembayaran ganti kerugian kepada pelaku usaha. Perampasan keuntungan dari tindak pidana.Pencabutan hak tertentu (seperti jabatan publik) (Undang-Undang Nomor 27 Tahun 2022).

D. KESIMPULAN

Tindakan pejabat yang melanggar data pribadi dengan menyalahgunakan hak akses digital ke orang lain atau ke publik tidak dibenarkan undang-undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. Kasus I Made pejabat di Buleleng menjadi contoh bahwa pejabat tidak boleh menyalahgunakan kewenangannya untuk menghambat proses penerbitan izin yang dilakukan dalam sistem elektronik *Online Single Submission* (OSS) dengan alasan untuk keuntungan pribadi, meskipun I Made Divonis atau dihukum dengan hukuman pemerasan dan korupsi dengan menyalahgunakan jabatan karena yang menjadi titik utama kasusnya, tetapi dalam penelitian ini membahas dari sisi penyalahgunaan hak akses data digital yang dilakukan pejabat yang menyalahgunakan jabatannya yang berlandaskan Undang-undang perlindungan data pribadi, sebagai bagian yang juga sangat penting untuk

dibahas agar kedepannya bisa memberikan masukan bagi aparat penegak dalam mempertimbangkan vonis atau hukuman bagi kasus yang serupa.

E. REFERENSI

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022.

Arman, Z., & Riyanda, R. (2022). Administrative Penal Law dalam Penegakan Hukum Lingkungan Berdasarkan Undang-Undang Cipta Kerja. Jurnal Hukum Samudra Keadilan, 17(2), 243. ejurnalunsam.id (Diakses pada 20 Juli 2026).

Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Perlindungan Data Pribadi di Indonesia. Jurnal Hukum Lex Generalis, 2(8), 652. https://rewangrencang.com (Diakses pada 20 Juli 2026).

Muslim. (2020). Asas Primum Remedium dalam Penegakan Hukum Pidana di Bidang Lingkungan Hidup. Eksekusi: Journal of Law, 2(1), 44. http://uin-suska.ac.id (Diakses pada 20 Juli 2026).

(Antara News Bali. (2025). Kadis DPMPTSP Buleleng jadi tersangka dugaan pemerasan pengembang. Antaranews.com. (Diakses pada 20 Juli 2026).

JDIH BPK Perwakilan Provinsi Bali. (2025, 25 Maret). Kadis PMPTSP Buleleng Tersangka Kasus Pemerasan. Catatan Berita Hukum. bpk.go.id (Diakses pada 20 Juli 2026).

Mahendro, A. (2025, 20 Maret). Kadis DPMPTSP Buleleng Diduga Peras Pengembang Rumah Subsidi. DetikBali. https://detik.com (Diakses pada 20 Juli 2026).